BANCO CENTRAL DO BRASIL - BRASÍLIA

Estudo Técnico Preliminar 115/2025

1. Informações Básicas

Número do processo: 284825

2. Descrição da necessidade

O Banco Central do Brasil (BCB), uma autarquia de natureza especial dotada de autonomia técnica, operacional, administrativa e financeira, desvinculada de qualquer ministério, tem como objetivo principal assegurar a estabilidade de preços. Para cumprir este mandato primordial e, sem prejuízo dele, perseguir seus objetivos secundários, o BCB desempenha um conjunto complexo e essencial de atividades.

Os objetivos secundários incluem zelar pela estabilidade e pela eficiência do sistema financeiro, suavizar as flutuações do nível de atividade econômica e fomentar o pleno emprego. A consecução desses objetivos exige uma atuação robusta e especializada nas seguintes frentes:

1. **Controle da Inflação:** Através da execução da política monetária, notadamente pela definição da taxa básica de juros (Selic) via Comitê de Política Monetária (Copom), o BCB busca atingir as metas para a inflação (definidas pelo Conselho Monetário Nacional - CMN), preservando o valor da moeda nacional e o poder de compra dos cidadãos.
2. **Estabilidade e Eficiência Financeira:** O BCB exerce a supervisão do sistema financeiro, monitorando riscos, regulando e garantindo o cumprimento de normas pelas instituições, promovendo a solidez, a eficiência e a segurança das transações e da intermediação financeira no país.
3. **Suavização de Ciclos Econômicos e Fomento ao Emprego:** As políticas implementadas pelo BCB visam contribuir para um ambiente macroeconômico estável, atenuando oscilações bruscas na atividade econômica e favorecendo as condições para a geração de emprego e renda.
4. **Infraestrutura do Mercado Financeiro:** O BCB regula, supervisiona e, em alguns casos, opera componentes críticos da infraestrutura do mercado financeiro, como os sistemas de pagamentos (incluindo o Pix), garantindo sua funcionalidade, segurança e evolução contínua.
5. **Prestação de Contas e Transparência:** O BCB cumpre rigorosos ritos de prestação de contas, incluindo a apresentação de relatórios periódicos ao Senado Federal, e divulga amplamente suas decisões, análises e dados econômicos.
6. **Atuação Internacional:** O BCB representa o Brasil em fóruns econômicos e financeiros globais, buscando a convergência com as melhores práticas internacionais e a estabilidade financeira global.

Adicionalmente, a crescente digitalização dos serviços financeiros e a própria atuação do BCB em um ambiente tecnológico complexo impõem desafios significativos. Devido ao universo quase imensurável da rede web atual, onde circulam infinitas informações, é necessário o emprego de alta tecnologia para que seja possível detectar ameaças e comportamentos suspeitos direcionados contra o BCB, seus ativos, processos e atividades. A crescente interdependência entre o mundo físico e o digital tem ampliado significativamente o espectro de riscos enfrentados pelas instituições públicas. Manifestações físicas, por exemplo, muitas vezes são articuladas previamente em redes sociais e aplicativos de mensagens, onde grupos organizados compartilham estratégias, locais e horários de ação. Essa coordenação digital pode potencializar ameaças físicas, como invasões, sabotagens ou bloqueios, ao mesmo tempo em que dificulta a antecipação por parte dos órgãos de segurança. Assim, a proteção contra essas ameaças — tanto físicas quanto virtuais — torna-se vital para a manutenção da estabilidade institucional, da confiança no sistema financeiro e da integridade das operações da Autarquia.

Para atingir tal objetivo de segurança e resiliência física e virtual, são necessários conhecimentos altamente especializados, atualização constante, atuação dinâmica e eficaz, bem como capilaridade, demandando grandes e variados esforços em termos de organização, orquestração e governança de processos, pessoas e ferramentas tecnológicas avançadas.

Considerando a centralidade das atribuições do BCB para a saúde econômica do país, a complexidade técnica exigida para sua execução autônoma e eficiente, e os desafios impostos pelo ambiente digital e de segurança física e virtual, a presente contratação é indispensável para prover a prestação de serviços continuados de OSINT (Open Source Intelligence) e Social Listening para contrainteligência e monitoramento da web (surface, deep e dark web). Esta iniciativa está diretamente alinhada ao Plano Diretor de Segurança (PDS 2024-2029) do BCB, especialmente ao Indicador 06, que prevê a otimização do monitoramento de ameaças mediante ferramentas automatizadas de análise de fontes abertas e inclusão de dados prospectivos nos relatórios de contrainteligência. Tais serviços são cruciais para capacitar o BCB na identificação e análise proativa de informações relevantes e na detecção de ameaças,

narrativas adversas, comportamentos suspeitos, campanhas de desinformação e outras atividades no ambiente digital que possam impactar negativamente seus ativos, processos, imagem institucional, a estabilidade do sistema financeiro ou a segurança de suas operações, conforme os desafios de segurança e contrainteligência anteriormente mencionados. A falta ou inadequação destes serviços especializados de contrainteligência e monitoramento da web representaria uma vulnerabilidade crítica, comprometendo a capacidade do BCB de antecipar, compreender e mitigar riscos oriundos do ciberespaço, proteger seus ativos e informações, e garantir a continuidade de suas operações críticas de forma autônoma e segura.

2.1 Ativos Específicos para Monitoramento

Para atender às necessidades de segurança e contrainteligência do Banco Central do Brasil, deverão ser monitorados especificamente:

1. **Manifestações sociais contra o BCB**
    - Mobilizações em redes sociais e grupos de mensagens
    - Convocações para protestos ou ações hostis
    - Narrativas e discursos contra a instituição ou suas políticas
2. **Criminosos ou grupos com atuação em crimes contra instituições financeiras**
    - Identificação de indivíduos ou organizações com histórico de ataques
    - Monitoramento de comunicações realizadas na web (surface, deep e dark web) sobre o planejamento de ações hostis contra o Banco Central do Brasil (BCB), bem como contrarias a marcas, produtos e iniciativas vinculadas à Autarquia, tais como o Pix, o sistema Valores a Receber, moedas comemorativas e outras ações institucionais de grande visibilidade. A análise deve contemplar conteúdos que indiquem intenções de ataques cibernéticos, campanhas de desinformação, incitação à violência ou mobilizações físicas articuladas digitalmente, considerando o potencial de repercussão e impacto reputacional.
    - Mapeamento de redes criminosas especializadas em crimes financeiros
3. **Ameaças contra operações e processos de trabalho**
    - Menções ameaçadoras a sistemas críticos operados pelo BCB
    - Discussões sobre vulnerabilidades em processos operacionais do BCB com a finalidade de explorá-las
    - Planejamento de ações para interrupção de serviços ou operações
4. **Ameaças contra instalações**
    - Menções ameaçadoras contra a sede e as representações regionais do BCB
    - Planejamento de invasões ou ataques físicos
    - Reconhecimento e mapeamento de instalações por potenciais ameaças

Desta forma, a contratação visa atender à necessidade de monitoramento, coleta e análise de informações de fontes abertas e mídias sociais para subsidiar atividades de:

- Proteção da imagem institucional;
- Monitoramento de ameaças físicas e virtuais contra ativos do BCB;
- Identificação preventiva de riscos reputacionais;
- Análise de tendências e comportamentos relevantes para a segurança institucional;
- Identificação de perfis e conteúdo que possam representar ameaças contra os ativos institucionais;
- Produção de relatórios de contrainteligência baseados em fontes abertas da web (surface, deep e dark web).

2.2 Motivação/Justificativa

O presente Estudo Técnico Preliminar tem por objetivo realizar o diagnóstico da necessidade de contratação de serviço especializado em OSINT (Open Source Intelligence) e Social Listening, demonstrando a viabilidade técnica e econômica da contratação, em conformidade com o disposto no art. 18, § 1º, da Lei nº 14.133, de 1º de abril de 2021.

3. Área requisitante

Área Requisitante	Responsável
Coordenação de Riscos e Inteligência do Departamento de Segurança	Aroldo Ferraz

4. Necessidades de Negócio

4.1 Descrição da Solução Como Um Todo

A solução proposta compreende a contratação de empresa especializada para prestação de serviços continuados de OSINT (Open Source Intelligence) e Social Listening, oferecendo um sistema abrangente de monitoramento, análise e resposta estratégica.

Esta solução contempla:

Infraestrutura e Plataforma

- Implementação de plataforma avançada para monitoramento sistemático de fontes abertas e mídias sociais, com capacidade de processamento em tempo real
- Acesso a ferramentas analíticas de última geração para identificação de padrões e anomalias em grandes volumes de dados (ex. inteligência artificial)
- A solução deverá prover uma console e o fornecimento de licenças de acesso para 14 usuários intercambiáveis, permitindo realocação de credenciais conforme necessidade operacional, mediante solicitação formal de desativação/ativação

Serviços Especializados

- Disponibilização de serviço de equipe técnica altamente qualificada para análise aprofundada das informações coletadas
- Suporte consultivo permanente para interpretação de resultados e direcionamento estratégico

Produtos de Contrainteligência

- Entrega de relatórios diários, semanais e mensais detalhando tendências emergentes, potenciais ameaças e situações críticas identificadas

Sistema de alertas em tempo real para situações de crise, com relatórios *ad hoc* imediatos

- Mapeamento detalhado de redes de influência e vetores de propagação de informações relevantes ou desinformação

Capacidades Analíticas Avançadas

- Desenvolvimento de análises preditivas baseadas em histórico de dados e tendências comportamentais
- Identificação proativa de riscos potenciais antes que se transformem em crises

Transferência de Conhecimento

- Programa estruturado de treinamento para capacitação da equipe interna na utilização eficiente das ferramentas disponibilizadas
- Workshops periódicos de atualização sobre novas técnicas e metodologias de análises

Esta solução permitirá à organização antecipar-se a cenários adversos, proteger sua reputação e fundamentar decisões estratégicas com base em contrainteligência acionável e confiável.

A solução compreende a prestação de serviços continuados de OSINT e Social Listening, englobando:

1. Plataforma Tecnológica:

- Sistema de monitoramento de fontes abertas e mídias sociais

- Ferramentas de coleta, processamento e análise de dados

- Dashboard customizável para visualização de informações

- Sistema de alertas configuráveis

- Módulo de geração de relatórios

- Console para login de usuários

2. Equipe Técnica Especializada:

- Gerente de Projeto

- Coordenador de Contrainteligência

- Analistas de Dados para Contrainteligência

- Analista de Redes

- Analista de OSINT Sênior

- Analista de OSINT Júnior

- Analista de Ameaças

- Especialista em Social Listening

- Especialista em Ferramentas de OSINT e Social Listening

- Especialista em IA para Contrainteligência

3. Serviços de Monitoramento:

- Coleta contínua de dados de fontes abertas

- Monitoramento de palavras-chave, perfis e hashtags definidos

- Acompanhamento de tendências e comportamentos

- Análise de sentimento e engajamento

- Análise com técnicas avançadas (Capacidades Avançadas de Detecção e Identificação; Capacidades de Análise Contextual Aprimorada; Capacidades Preditivas e Preventivas; Capacidades Multilíngues e Multimodais e Capacidades de Contrainteligência Digital)

4. Produtos e Entregas:

- Relatórios diários de monitoramento

- Relatórios semanais analíticos

- Relatórios mensais estratégicos

- Alertas em tempo real para situações críticas

- Análises específicas sob demanda

- Console para login de até 14 usuários

4.2 Escopo da Contratação

O escopo da contratação abrange:

1. Fontes a serem monitoradas:

- Redes sociais: X, Facebook, Instagram, LinkedIn, YouTube, TikTok

- Plataformas de mensagens: Telegram (grupos públicos), WhatsApp (grupos públicos), Discord.

- Fóruns e comunidades online

- Blogs e sites de notícias

- Plataformas de vídeo e streaming (ex. Vimeo, Youtube)

- Repositórios públicos de documentos

- Deepweb

- Darkweb

2. Temas e ativos para monitoramento:

- Manifestações sociais contra o BCB, incluindo protestos planejados ou em andamento

- Criminosos ou grupos com atuação em crimes contra instituições financeiras

- Ameaças físicas e digitais contra operações e processos de trabalho do BCB

- Ameaças físicas e digitais contra instalações do Banco Central do Brasil

- Vazamentos de dados sensíveis relacionados à instituição

- Campanhas de desinformação direcionadas ao BCB ou ao sistema financeiro

- Menções ameaçadoras a vulnerabilidades de segurança do BCB ou de seus sistemas

- Planejamento de ataques cibernéticos ou físicos contra a instituição

3. Tipos de análise requeridos:

- Análise de sentimento

- Análise de engajamento e alcance

- Análise de redes e conexões

- Análise de tendências temporais

- Identificação de influenciadores

- Detecção de padrões anômalos

- Análise georreferenciada

- Análise de vazamentos e exposição de informação sensível

5. Necessidades Tecnológicas

5.1 Infraestrutura Tecnológica

1. Plataforma integrada de monitoramento capaz de coletar, processar e analisar dados de múltiplas fontes abertas, incluindo redes sociais, sites de notícias, blogs, fóruns e comunidades online.
2. Sistema de gestão de acessos para administração de 14 usuários intercambiáveis na plataforma principal, com mecanismos para transferência de credenciais conforme necessidade operacional.
3. Infraestrutura de alta disponibilidade com redundância, processamento escalável e capacidade de armazenamento suficiente para atender ao volume projetado de dados.
4. Mecanismos de backup e recuperação para garantir a continuidade da operação e a preservação dos dados históricos pelo período contratual.
5. Arquitetura flexível que permita adaptação a novos requisitos e incorporação de fontes adicionais ao longo da vigência contratual.

5.2 Capacidades Analíticas

1. Ferramentas de Processamento de Linguagem Natural (PLN) com capacidade multilíngue e análise contextual avançada, especialmente para o português brasileiro.
2. Sistemas de inteligência artificial para detecção de anomalias, análise de sentimento, reconhecimento de padrões e identificação de atividades coordenadas inautênticas.
3. Recursos de visualização de dados que permitam representações gráficas de redes de relacionamento, análises temporais, georreferenciamento e tendências estatísticas.
4. Mecanismos de correlação entre diferentes fontes de informação para identificação de padrões complexos e ameaças emergentes.
5. Capacidades preditivas baseadas em modelos de aprendizado de máquina para identificação precoce de riscos potenciais.

5.3 Ferramentas de Operação

1. Sistema de alertas configuráveis com múltiplos canais de notificação (e-mail, SMS, aplicativo) para situações críticas identificadas.
2. Interface de usuário intuitiva com dashboards personalizáveis, visualizações interativas e navegação contextual.
3. Ferramentas de pesquisa avançada com suporte a operadores booleanos, expressões regulares e busca semântica.
4. Recursos de exportação de dados em formatos padronizados (CSV, PDF, XLSX, JSON, H5 e DOCX) para integração com outros sistemas.

5. Funcionalidades de workflow para gerenciamento do ciclo de vida das ameaças identificadas, desde a detecção até a mitigação.

5.4 Recursos Humanos Especializados

1. Equipe multidisciplinar composta por especialistas em OSINT, análise de dados, mídias sociais, análise de redes e inteligência artificial.
2. Profissionais com experiência comprovada no monitoramento de ameaças direcionadas a instituições financeiras e infraestruturas críticas.
3. Especialista dedicado em inteligência artificial para desenvolvimento e implementação de modelos analíticos avançados específicos para o contexto do BCB.
4. Analistas de contrainteligência com capacidade para identificar tentativas de reconhecimento hostil e proteção de informações sensíveis.
5. Capacidade de produção de análises estratégicas que traduzam dados técnicos em informações acionáveis para tomada de decisão.

5.5 Segurança e Conformidade

1. Controles de segurança robustos incluindo criptografia de dados, autenticação multifator (2FA), segmentação lógica e monitoramento de atividades.
2. Conformidade com regulamentações aplicáveis ao setor financeiro, com especial atenção à Lei Geral de Proteção de Dados (LGPD) e às normas do Banco Central.
3. Procedimentos de resposta a incidentes para garantir a integridade e disponibilidade da plataforma e dos dados.
4. Proteção contra vazamento de informações sensíveis através de controles técnicos e compromissos de confidencialidade.
5. Mecanismos de auditoria que permitam rastreabilidade completa de todas as ações realizadas na plataforma.

5.6 Produtos e Entregas

1. Relatórios periódicos (diários, semanais e mensais) com diferentes níveis de profundidade analítica e focos específicos.
2. Alertas em tempo real para situações críticas ou de alto impacto potencial.
3. Análises sob demanda para temas específicos ou cenários emergentes.
4. Feedbacks para refinamento contínuo dos parâmetros de monitoramento.
5. Transferência de conhecimento por meio de capacitação da equipe interna do BCB na utilização eficiente das ferramentas disponibilizadas.

Plano de Capacitação compreendendo treinamento anual de 40 horas para cada membro da equipe especializada da contratada, garantindo atualização constante sobre novas técnicas, ferramentas e metodologias.

6. Demais requisitos necessários e suficientes à escolha da solução de TIC

Com base na análise da demanda e nos documentos de referência apresentados, foram identificados os seguintes requisitos complementares essenciais para a adequada seleção e contratação da solução de TIC:

6.1 Requisitos de Integração e Interoperabilidade

A solução deverá permitir integração com sistemas existentes no BCB através de *Application Programming Interface* (APIs) padronizadas, possibilitando o compartilhamento de dados e informações de forma segura e controlada. Deve suportar formatos de exportação padrão como CSV, XML, JSON e PDF para facilitar a interoperabilidade com outras ferramentas de análise utilizadas pelo Tribunal.

6.2 Requisitos de Capacidade e Performance

A plataforma deve suportar operação simultânea de múltiplos usuários (mínimo de 14 usuários concorrentes) sem degradação significativa de performance. O tempo de resposta para consultas simples não deve exceder 5 segundos, enquanto consultas complexas com grande volume de dados devem ser processadas em até 30 segundos.

6.3 Requisitos de Backup e Continuidade

A solução deve implementar rotinas automáticas de backup dos dados coletados e configurações do sistema, com frequência mínima diária. Em caso de falha, o sistema deve ser restaurado em prazo máximo de 4 horas, garantindo a continuidade dos serviços essenciais do BCB.

6.4 Requisitos de Auditoria e Rastreabilidade

O sistema deve manter logs detalhados de todas as operações realizadas, incluindo consultas executadas, usuários responsáveis, *timestamps* e resultados obtidos. Estes logs devem ser preservados por período mínimo de 5 anos e estar disponíveis para auditoria sempre que solicitado.

6.5 Requisitos de Customização e Configuração

A solução deve permitir configuração de parâmetros específicos para o BCB, incluindo personalização de dashboards, definição de alertas customizados baseados em palavras-chave específicas do órgão, e criação de relatórios adaptados às necessidades institucionais.

6.6 Requisitos de Garantia e Suporte Técnico

Garantia da Solução: A solução contratada deve possuir garantia integral pelo período de 12 meses, cobrindo defeitos de funcionamento, falhas de software e problemas de configuração. A garantia deve incluir correção de bugs identificados e atualizações de segurança sem custo adicional.

Suporte Técnico Especializado: Deve ser disponibilizado suporte técnico em idioma português, com atendimento por meio de múltiplos canais (telefone, e-mail, chat online e sistema de tickets). O suporte deve funcionar em horário comercial (8h às 18h, segunda a sexta-feira) com tempo de resposta máximo de 4 horas para questões críticas e 24 horas para questões não-críticas.

6.7 Requisitos de Manutenção e Assistência Técnica

Manutenção Preventiva: A contratada deve realizar manutenções preventivas programadas mensalmente, incluindo otimização de performance, limpeza de bases de dados temporárias e verificação de integridade do sistema. Estas manutenções devem ser comunicadas com antecedência mínima de 48 horas.

Manutenção Corretiva: Em caso de falhas ou defeitos identificados, a contratada deve disponibilizar correções em prazo máximo de 24 horas para problemas críticos que afetem a disponibilidade do sistema, e 72 horas para problemas não-críticos.

Assistência Técnica Remota: A solução deve permitir assistência técnica remota segura, com sessões monitoradas e registradas, respeitando as políticas de segurança da informação do BCB.

6.8 Requisitos de Evolução e Atualização

A solução deve receber atualizações regulares de funcionalidades, bases de dados e mecanismos de coleta, sem custo adicional durante o período contratual. As atualizações devem ser compatíveis com versões anteriores e não devem interromper o funcionamento normal do sistema por período superior a 2 horas.

6.9 Requisitos de Documentação e Treinamento

Deve ser fornecida documentação técnica completa em português, incluindo manuais de usuário, guias de administração e documentação de APIs. O treinamento inicial deve contemplar pelo menos 16 horas de capacitação para a equipe técnica do BCB, abordando tanto aspectos operacionais quanto administrativos da ferramenta.

6.10 Requisitos de Licenciamento e Propriedade Intelectual

O modelo de licenciamento deve ser transparente, especificando claramente os direitos de uso, limitações e responsabilidades de cada parte. Os dados coletados e processados pela solução devem permanecer sob propriedade do BCB, garantindo que não sejam utilizados pela contratada para outros fins que não a prestação do serviço contratado.

Estes requisitos, em conjunto com as especificações técnicas detalhadas nos itens anteriores, constituem o conjunto mínimo necessário para a adequada seleção e contratação da solução de tecnologia da informação que atenderá às necessidades do Banco Central do Brasil.

7. Estimativa da demanda - quantidade de bens e serviços

7.1 Dimensionamento dos Quantitativos

7.1.1 Premissas Fundamentais

1. **Cobertura territorial**: Consideração da presença do BCB em todo território nacional, com 10 sedes regionais e operações descentralizadas em 27 unidades da federação.
2. **Universo de ativos**: Mapeamento abrangente dos ativos críticos do BCB, incluindo instalações físicas, operações especializadas e reputação institucional.
3. **Complexidade operacional**: Reconhecimento da diversidade de operações do BCB, desde atividades regulatórias até operações físicas como transporte de numerário e funcionamento de delegacias regionais.
4. **Benchmarking interno**: Utilização da experiência prévia do BCB em contratações similares (como a contratação de CTI pelo Deinf) como referência para dimensionamento.

7.2 Fórmulas de Cálculo:

- Para ameaças geográficas dispersas: Quantidade = Número de UFs + Margem de segurança (%)

- Para instalações e operações: Quantidade = Sedes fixas + Localidades de operação

7.3 Parâmetros de Entrada

- **27 Unidades da Federação**: Base territorial para monitoramento de grupos criminosos regionalizados
- **10 Sedes do BCB**: Instalações fixas com presença física permanente
- **40 Cidades com operações**: Locais onde ocorrem atividades e operações
- **13 Instalações críticas**: Sedes principais e instalações de alta relevância estratégica
- **14 Usuários intercambiáveis**, permitindo realocação de credenciais conforme necessidade operacional, mediante solicitação formal de desativação/ativação

Item	Descrição	Ativos Monitorados	Base de Cálculo	Quantidade
1	Monitoramento de manifestações sociais contra o BCB	Reputação do BCB	Cobertura nacional + eventos regionais específicos	36
2	Monitoramento de criminosos ou grupos com atuação em crimes contra instituições financeiras	Numerário do BCB	27 UFs (cobertura por estado)	27
3	Monitoramento de ameaças contra operações e processos de trabalho	Operações e processos de trabalho do BCB	Cidades com operações e Sedes	40
4	Monitoramento de Ameaças contra instalações	Instalações do BCB	Sedes principais e instalações críticas	13
5	Usuários intercambiáveis, permitindo realocação de credenciais conforme necessidade operacional, mediante solicitação formal de desativação/ativação	-	-	14

7.4 Justificativas Específicas

Item 1 (Manifestações sociais - 36 unidades): Considera monitoramento nacional (27 UFs) acrescido de 10 grandes centros urbanos com maior concentração de ativismo, baseado em dados históricos de manifestações contra o Banco Central.

Item 2 (Grupos criminosos - 27 unidades): Um ponto de monitoramento por Unidade da Federação, considerando que grupos criminosos especializados em crimes financeiros tendem a ter atuação regionalizada.

Item 3 (Operações - 40 unidades): Soma das cidades com operações (30) e sedes (10), considerando que estas atividades representam os pontos de maior exposição operacional.

Item 4 (Instalações - 13 unidades): Compreende as 10 sedes regionais do BCB acrescidas de 3 instalações de importância estratégica nacional (sede em Brasília e instalações críticas em São Paulo e Rio de Janeiro).

Item 5 (14 usuários intercambiáveis): Quantitativo de servidores do BCB com permissões de uso da ferramenta, com possibilidade de realocação de credenciais conforme necessidades operacionais, mediante solicitação formal de ativação ou desativação de acessos.

7.5 Produtos e Entregas

A solução resultará na entrega de produtos customizados conforme os quantitativos dimensionados, incluindo relatórios específicos para cada categoria de ativo monitorado, alertas direcionados e análises contextualizadas que permitam ao BCB uma visão integrada do panorama de ameaças e riscos identificados através de fontes abertas.

8. Levantamento de soluções

O presente levantamento visa identificar e analisar as diferentes alternativas disponíveis para atendimento da demanda de serviços de OSINT (*Open Source Intelligence*) e Dark Web Intelligence, considerando aspectos técnicos, operacionais, econômicos e de viabilidade para implementação no contexto da Segurança Pública e Inteligência Governamental.

8.1 Contexto de Mercado e Tendências

A Administração Pública Federal brasileira investiu mais de R$ 400 milhões em serviços de inteligência de fontes abertas e monitoramento de mídias sociais entre 2017-2024, revelando um mercado concentrado em poucas empresas especializadas e caracterizado por contratações estratégicas por razões de "segurança nacional".

O mercado global de *open source intelligence*, avaliado em $5,02 bilhões em 2018, está previsto para crescer para $29,19 bilhões até 2026, com uma taxa de crescimento anual composta (CAGR) de 24,7% de 2020 a 2026, demonstrando a crescente importância estratégica dessas tecnologias para organismos de segurança e inteligência.

8.1.1 Estrutura da Internet e Necessidades de Monitoramento

As soluções de OSINT atuam em três camadas distintas da internet, cada uma com características específicas que demandam capacidades tecnológicas diferenciadas:

Surface Web (Internet Superficial)

- Conteúdo prontamente acessível e indexado por mecanismos de busca padrão
- Constitui menos de 5% do conteúdo total da internet
- Inclui redes sociais, sites de notícias, fóruns públicos e plataformas de mídia

Deep Web (Internet Profunda)

- Abrange todo o conteúdo não indexado por mecanismos de busca tradicionais
- Inclui bancos de dados universitários, repositórios acadêmicos, portais protegidos por senha
- Plataformas de comunicação corporativa e sistemas de gestão interna

Dark Web (Internet Obscura)

- Subseção intencional e deliberadamente oculta da deep web
- Acessível exclusivamente através de tecnologias de anonimização como Tor Browser, I2P e Freenet
- Concentra atividades ilícitas, mercados clandestinos e comunicações criminosas
- Representa o maior desafio investigativo e é um dos principais objetivos desta contratação

8.2 Metodologia de Levantamento

Para construção do panorama de soluções disponíveis, foram realizadas as seguintes ações de levantamento conforme diretrizes do art. 11 da Lei nº 14.133/2021 e Instrução Normativa SGD/ME nº 94/2022:

8.2.1 Necessidades Similares na Administração Pública

Foi conduzido levantamento abrangente junto a órgãos da Administração Pública Federal e Estaduais com demandas similares, identificando-se as seguintes experiências relevantes e benchmarks de mercado:

Secretaria Nacional de Segurança Pública (SENASP/MJSP)

- **Escopo**: Contratação de solução para investigação em Dark Web com funcionalidades de monitoramento de fóruns, mercados clandestinos e vazamentos de dados
- **Modalidade**: Sistema de Registro de Preços (SRP) com participação de múltiplos órgãos estaduais
- **Valor**: R$ 14.392.500,00 para 19 licenças com suporte técnico integral de 36 meses
- **Especificações**: Plataforma SaaS com capacidades de navegação anônima, análise de correlação e alertas automatizados

Tribunal de Contas do Distrito Federal (TCDF)

- **Escopo**: Subscrição de Solução Tecnológica de Segurança Corporativa na modalidade SaaS
- **Valor**: R$ 767.534,64 para 12 meses
- **Componentes**: Solução de Coleta e Processamento de Dados (R$ 478.646,64) + Solução de Coleta em Fontes Abertas (R$ 288.888,00)
- **Características**: Baseada em coleta e integração de dados em fontes abertas com ênfase no monitoramento de infraestrutura

Receita Federal do Brasil (RFB)

- **Escopo**: Subscrição SNAP-DESKTOP (OSINT + Maltego + Credilink + Social Link)
- **Valor**: R$ 4.063.352,40 para 30 licenças anuais (R$ 135.445,08 por licença)
- **Adicional**: Treinamento Fundamentos SNAP-EAD (R$ 18.034,22 para 6 participantes)
- **Características**: Localização, transformação e apresentação de dados coletados de fontes públicas, comerciais e privadas

Polícia Civil do Estado de São Paulo (DIPOL)

- **Escopo**: Aquisição de software analítico especializado i2 (Analyst's Notebook, iBase, Analysis Studio)
- **Valor**: R$ 80.050.747,32 para licenças e treinamentos especializados
- **Foco**: Análise de vínculos, investigação criminal e visualização de redes criminosas
- **Modalidade**: Licenças perpétuas com suporte técnico estendido

Ministério Público do Distrito Federal e Territórios (MPDFT)

- **Escopo**: Contratação de solução para monitoramento e extração de inteligência de mídias sociais e fontes abertas, incluindo Deep e Dark Web, com serviços de assistência técnica e treinamento.
- **Modalidade**: Inexigibilidade de licitação, conforme contrato nº 082/PGJ/MPDFT/2020.
- **Valor**: R$ 9.225.860,78 (6 licenças on-premise perpétuas / 36 meses).
- **Especificações**:
  - Solução de inteligência com funcionalidades de coleta e análise de dados em mídias sociais, fóruns e ambientes da deep /dark web.
  - Entrega da solução em até 120 dias após assinatura do contrato.
  - Treinamento técnico a ser realizado até 30 dias após a entrega da solução.
  - Atendimento técnico com prazo de solução de chamados em até 48 horas.
  - Entregas previstas: reunião de alinhamento, plano de treinamento, recebimento provisório e definitivo da solução.

8.2.2 Alternativas do Mercado

O mercado nacional e internacional oferece diferentes categorias de soluções para OSINT e Dark Web Intelligence, cada uma com características específicas de implementação e custos:

Soluções Integradas Comerciais (Tier 1)

- Plataformas proprietárias com funcionalidades completas de monitoramento Dark Web
- Capacidade de coleta automatizada em fóruns, mercados, canais Telegram/Discord, plataformas peer-to-peer
- Licenciamento baseado em número de usuários concorrentes (1-50 usuários)
- Suporte técnico 8x5 com atualizações inclusas e patches de segurança
- Principais fornecedores: Sixgill, DarkOwl, Recorded Future, Flashpoint
- Custo estimado: R$ 500.000 - R$ 1.200.000 por licença/ano

Soluções Especializadas em Investigação (Tier 2)

- Software i2 (IBM): Analyst's Notebook, iBase, Analysis Studio
- Preços unitários: R$ 32.666,67 (iBase) a R$ 178.062,07 (Analysis Studio) por licença
- Treinamentos especializados: 30-42 horas de capacitação por produto
- Foco principal: análise de vínculos, visualização de redes criminosas e inteligência tática
- Limitação: Não específico para Dark Web, requer integração com outras ferramentas

Soluções SaaS (Software as a Service) - Tier 3

- Fornecimento via nuvem com infraestrutura própria do fornecedor
- Acesso através de navegador web e aplicativos móveis dedicados
- Autenticação multifator (2FA/MFA) obrigatória com logs de auditoria
- Armazenamento seguro em data centers certificados (ISO27001, SOC2)
- Vantagens: Implementação rápida, atualizações automáticas, redução de custos de infraestrutura

Soluções Híbridas (Produto + Serviço) - Tier 4

- Combinação de plataforma tecnológica com serviços analíticos especializados
- Equipe técnica dedicada para interpretação contextualizada e análise humanizada
- Transferência de conhecimento em modalidades EAD "on-demand" ou presencial "hands-on"
- Aplicação: Adequado para organizações sem expertise interna prévia

8.2.3 Softwares Disponíveis no Governo (Portaria STI/MP nº 46/2016)

Conforme validado nos estudos da SENASP e por consulta direta ao Portal do Software Público Brasileiro, foi realizada pesquisa com os termos "dark web", "OSINT", "inteligência", "investigação" e "monitoramento", resultando nos seguintes achados:

Limitações Identificadas:

- Ausência completa de ferramentas especializadas em monitoramento Dark Web
- Falta de capacidades analíticas avançadas para investigação e levantamentos de contrainteligência
- Inexistência de recursos para navegação segura em redes Tor/Onion
- Ausência de sistemas de correlação de dados para inteligência e contrainteligência
- Falta de interfaces adequadas para análise de grandes volumes de dados estruturados e não estruturados

Conclusão: O Portal do Software Público Brasileiro não dispõe de soluções adequadas às necessidades específicas de OSINT e Dark Web Intelligence, conforme também identificado pela SENASP em seus estudos técnicos.

8.2.4 Políticas, Modelos e Padrões de Governo

A adoção de soluções tecnológicas por instituições brasileiras deve observar rigorosamente uma série de aspectos legais, técnicos e operacionais, respeitando as políticas, modelos e padrões definidos pelo governo federal.

Aspectos Legais e Normativos

- LGPD (Lei nº 13.709/2018): Conformidade com princípios de proteção de dados pessoais, minimização de coleta e finalidade específica
- LAI (Lei nº 12.527/2011): Equilíbrio entre transparência governamental e necessário sigilo operacional
- Marco Civil da Internet (Lei nº 12.965/2014): Respeito à neutralidade da rede e privacidade dos usuários
- Decreto nº 9.637/2018: Política Nacional de Segurança da Informação (PNSI)
- Instrução Normativa GSI/PR nº 1/2019: Metodologia de Gestão de Riscos de Segurança da Informação

Aspectos Técnicos e Arquiteturais

- e-PING: Padrões de Interoperabilidade de Governo Eletrônico para integração sistêmica
- e-MAG: Modelo de Acessibilidade em Governo Eletrônico para interfaces inclusivas
- ISO 27001: Gestão de Segurança da Informação com controles específicos para dados sensíveis
- SOC 2: Auditoria de controles de segurança para provedores de serviços em nuvem
- NIST Cybersecurity Framework: Framework de cibersegurança para proteção de infraestruturas críticas

Infraestrutura e Hospedagem

- Preferência on-premise: Para tratamento de dados sensíveis e operações críticas
- Compatibilidade SISP: Sistema de Administração dos Recursos de Tecnologia da Informação
- Certificação ICP-Brasil: Para autenticação e assinatura digital em processos críticos

8.2.5 Políticas e Modelos de Contratação

Modalidades Recomendadas

- Sistema de Registro de Preços (SRP): Vigência mínima de 12 meses com possibilidade de prorrogação até 180 meses
- Pregão Eletrônico: Modalidade preferencial com critério de menor preço por lote
- Modo de Disputa: "Aberto e Fechado" para maximizar competitividade
- Verificação de Amostra: Obrigatória antes da contratação definitiva (art. 116, §§ 1º e 2º, Lei nº 14.133/2021)

Participação Multi-Órgãos Possibilidade de adesão por órgãos com necessidades similares, incluindo:

- Polícias Civis Estaduais e Distrital
- Polícias Militares e Corpo de Bombeiros
- Ministério Público Federal e Estaduais
- Receita Federal e órgãos de controle
- Agências reguladoras e de investigação

8.2.6 Tipologia de Soluções por Especificação e Composição

Solução Básica de Monitoramento (Nível 1)

- Funcionalidades: Monitoramento automatizado de fontes Dark Web predefinidas, alertas configuráveis para palavras-chave específicas, relatórios padronizados com periodicidade fixa
- Capacidade: 1-5 usuários concorrentes, 10.000 consultas mensais
- Limitações: Sem capacidade de correlação avançada ou análise contextual
- Estimativa: R$ 300.000 - R$ 500.000 anuais

Solução Intermediária com Análise (Nível 2)

- Funcionalidades: Capacidades de busca avançada com operadores especializados, análise de correlação entre identificadores, dashboard para visualização de dados coletados
- Capacidade: 5-15 usuários concorrentes, 50.000 consultas mensais
- Recursos: API para integração, exportação de dados, análise de tendências
- Estimativa: R$ 500.000 - R$ 750.000 anuais

Solução Avançada com Inteligência Artificial (Nível 3)

- Funcionalidades: IA para detecção de padrões complexos, análise de conteúdo relacionado aos ativos definidos no Edital
- Capacidade: 15-50 usuários concorrentes, consultas ilimitadas
- Recursos: Equipe especializada para análises contextualizadas, machine learning, processamento de linguagem natural e IA Generativa
- Estimativa: R$ 750.000 - R$ 1.200.000 anuais

9. Análise comparativa de soluções

9.1 Quadro comparativo das soluções levantadas

Órgão	Escopo	Modalidade	Valor	Especificações Técnicas	Resultado da Análise
SENASP /MJSP	Investigação em Dark Web com monitoramento de fóruns, mercados clandestinos e vazamentos de dados	Sistema de Registro de Preços (SRP) com múltiplos órgãos	R$ 14.392.500,00 (19 licenças / 36 80357)	Plataforma SaaS com navegação anônima, análise de correlação e alertas automatizados	Não atende

MPDFT	Monitoramento e extração de inteligência de mídias sociais, deep e dark web, com assistência técnica e treinamento	Inexigibilidade de licitação (Contrato nº 082/PGJ /MPDFT/2020)	R$ 9.225.860,78 (6 licenças on-premise perpétuas / 36 meses)	Solução com coleta e análise de dados em mídias sociais e ambientes da deep/dark web, entrega em até 120 dias, treinamento técnico e suporte com SLA de 48h	Não atende
Receita Federal	Subscrição de 30 licenças SNAP-DESKTOP (SNAP + Maltego + Credilink + Social Links) com suporte e treinamento	Inexigibilidade de licitação	R$ 4.081.386,62 (12 meses)	Solução integrada com análise gráfica de dados públicos, comerciais e privados, com 6 treinamentos EAD de 8h	Não atende
TCDF	Subscrição de solução SaaS de segurança corporativa com coleta em fontes abertas e monitoramento de infraestrutura	Pregão eletrônico, menor preço por lote	R$ 767.534,64 (12 meses)	Coleta e integração de dados em fontes abertas, com suporte contínuo e alertas	Não atende
DIPOL (PC-SP)	Aquisição de software analítico especializado (i2 Analyst's Notebook, iBase, Analysis Studio)	Licitação com licenças perpétuas	R$ 80.050.747,32	Foco em análise de vínculos, investigação criminal e visualização de redes criminosas	Não atende

9.2 Análise Técnica Detalhada da Solução Recomendada

9.2.1 Requisitos Funcionais Essenciais

Coleta e Indexação Avançada

- Capacidade de coletar dados de fóruns clandestinos, mercados dark web, canais criptografados (Telegram, Discord, Signal)
- Indexação automatizada de identificadores únicos: IDs, usernames, endereços IP, e-mails, carteiras de criptoativos
- Processamento inteligente de dados vazados (credenciais, informações de cartões de crédito, documentos)
- Monitoramento de pastes sites (Pastebin, Ghostbin) e repositórios de código (GitHub, GitLab)

Segurança e Navegação Protegida

- Ambiente de navegação completamente emulado (Sandbox) com isolamento total
- Operação anônima garantindo proteção institucional e dos operadores
- Autenticação multifator (2FA/MFA) com logs de auditoria completos
- Mascaramento de identidade e geolocalização através de múltiplos proxies

Análise e Correlação Inteligente

- Algoritmos de machine learning para identificação de usuários com múltiplos identificadores
- Análise forense de blockchains para rastreamento de carteiras e transações suspeitas
- Detecção automatizada de tráfego dark web (incoming/outgoing) relacionado aos ativos monitorados
- Correlação temporal de eventos e atividades suspeitas
- Emprego de Machine Learning, Deep Learning, IA Generativa e agentes inteligentes para monitoramento e reporte de ameaças aos ativos especificados.

Gestão e Controle Operacional

- Interface para criação e gestão de múltiplos casos investigativos simultâneos
- Sistema hierárquico de controle de acesso por níveis de usuário (analista, supervisor, administrador)
- Marcadores personalizáveis e sistema de alertas configuráveis
- Relatórios executivos e operacionais com exportação em múltiplos formatos

9.2.2 Qualificação Técnica dos Fornecedores

Requisitos Mínimos Obrigatórios

- Comprovação de no mínimo 02 atestados de capacidade técnica nos últimos 24 meses
- Certificação como distribuidor/revenda autorizada ou desenvolvimento próprio da solução
- Infraestrutura de suporte técnico em âmbito nacional com atendimento em português
- Conformidade comprovada com ISO 27001 (Segurança da Informação) e SOC 2 (Controles de Auditoria)
- Equipe técnica certificada com no mínimo 05 profissionais especializados

Garantias Técnicas Exigidas

- Período mínimo de 36 meses de suporte técnico e atualizações inclusas
- Tempo de resposta para correções críticas: máximo 10 dias úteis
- Disponibilidade da solução 24x7 com SLA mínimo de 99,5%
- Suporte técnico especializado 8x5 (segunda a sexta, 8h às 18h)
- Transferência de conhecimento obrigatória com no mínimo 40 horas de treinamento

9.3 Recomendação Técnica Final

Cenário Recomendado: Solução SaaS Avançada com IA

Justificativa Técnica Fundamentada

1. **Especialização Crítica**: Necessidade de expertise específica em Dark Web não disponível internamente nem no mercado nacional
2. **Segurança Institucional**: Ambiente controlado com navegação anônima e proteção total da identidade institucional
3. **Agilidade Operacional**: Implementação em 30-60 dias sem necessidade de desenvolvimento interno prolongado
4. **Custo-Benefício Comprovado**: Modelo SaaS reduz significativamente riscos operacionais e de obsolescência tecnológica
5. **Escalabilidade**: Capacidade de expansão conforme crescimento das demandas investigativas

Especificação Técnica Recomendada

- Solução tipo "Cerberus", "DarkOwl Vision" ou "Sixgill Investigative Portal" com funcionalidades completas
- Licenciamento por usuário concorrente (5-15 usuários iniciais)
- Período contratual: 36 meses com possibilidade de prorrogação por igual período
- Valor estimado: R$ 750.000 - R$ 1.200.000 por licença no período de 36 meses
- Inclusão obrigatória de treinamento especializado e transferência de conhecimento

Modelo de Contratação Otimizado

- **Modalidade**: Sistema de Registro de Preços (SRP) para maximizar economia de escala
- **Licitação**: Pregão Eletrônico com critério de menor preço por lote
- **Verificação**: Verificação obrigatória de amostra antes da contratação definitiva
- **Participação**: Abertura para adesão de múltiplos órgãos de segurança pública e investigação
- **Capacitação**: Transferência de conhecimento em modalidade EAD e presencial obrigatória

9.4 Benefícios Esperados e Impactos

Benefícios Operacionais Diretos

- Redução de 60-80% no tempo médio de investigação em casos envolvendo Dark Web
- Detecção precoce de ameaças e atividades ilícitas com antecedência de 30-90 dias
- Correlação automatizada de informações de múltiplas fontes investigativas
- Capacidade de monitoramento contínuo 24x7 de alvos e temas sensíveis

Benefícios Estratégicos Institucionais

- Fortalecimento significativo da atividade de Contrainteligência de Segurança Pública
- Ampliação da capacidade de enfrentamento ao crime organizado cibernético

- Integração sinérgica com sistemas existentes de segurança e investigação
- Desenvolvimento de expertise interna através de transferência de conhecimento

Benefícios Econômicos e de Gestão

- Compartilhamento de custos entre múltiplos órgãos participantes do SRP
- Redução substancial de riscos através do modelo SaaS especializado
- Aproveitamento de economia de escala com fornecedores especializados
- ROI estimado de 300-400% considerando casos resolvidos vs. investimento

10. Registro de soluções consideradas inviáveis

10.1 Análise de Viabilidade

Cenário A: Desenvolvimento Interno

Descrição: Desenvolvimento através da fábrica de software institucional existente

Análise de Viabilidade: **INVIÁVEL**

- Expertise Insuficiente: Ausência de conhecimento interno especializado em tecnologias Dark Web, redes Tor e protocolos de anonimização
- Investimento Proibitivo: Necessidade de contratação de especialistas, aquisição de infraestrutura específica e investimento em Pesquisa e Desenvolvimento (P&D)
- Tempo Incompatível: Desenvolvimento estimado em 18-24 meses versus urgência operacional de 3-6 meses
- Riscos Elevados: Falta de garantias quanto à eficácia e conformidade com padrões internacionais de segurança
- Inadequação Funcional: Softwares convencionais não atendem especificidades de navegação anônima e coleta em ambientes clandestinos, conforme requerido pela especificação do BCB.
- Precedente SENASP: Análise similar realizada pela SENASP chegou à mesma conclusão de inviabilidade

Cenário B: Locação de Software Convencional

Descrição: Contratação de licenças de uso temporário de ferramentas genéricas

Análise de Viabilidade: **INVIÁVEL**

- Oferta Inexistente: Mercado especializado não oferece modalidade de locação para ferramentas Dark Web que se ajuste às necessidades específicas do Banco Central
- Inadequação Funcional: Softwares convencionais não atendem especificidades de navegação anônima e coleta em ambientes clandestinos, conforme requerido pela especificação do BCB.
- Custos Elevados: Modelo de locação tradicional resultaria em custos 40-60% superiores ao SaaS especializado
- Dependência Crítica: Dependência contínua do fornecedor sem garantias de continuidade

Cenário C: Aquisição de Licenças Perpétuas

Descrição: Compra de licenças com direito de uso definitivo para ferramentas de análise

Análise de Viabilidade: **PARCIALMENTE VIÁVEL** (apenas para ferramentas complementares)

- Aplicabilidade Limitada: Viável apenas para software de análise de vínculos (como por exemplo: i2 Analyst's Notebook)
- Lacuna Funcional: Não atende necessidades específicas de Dark Web Intelligence e de contrainteligência requeridas pelo BCB
- Investimento Elevado: R$ 82.298,09 por licença i2 Analyst's Notebook + custos de suporte anual
- Obsolescência: Risco de obsolescência tecnológica sem atualizações contínuas
- Recomendação: Adequado como ferramenta complementar, não como solução principal

Cenário D: Contratação de Solução SaaS Especializada

Descrição: Software como Serviço com funcionalidades completas para *Dark Web Intelligence* contendo recursos avançados de inteligência artificial e agentes inteligentes

Análise de Viabilidade: **ALTAMENTE RECOMENDADO**

- Especialização Comprovada: Soluções desenvolvidas especificamente para investigação e contrainteligência ajustadas às necessidades de uso do Banco Central
- Implementação Ágil: Disponibilização em 30-90 dias após contratação
- Custo-Benefício Otimizado: Modelo SaaS reduz custos de infraestrutura e manutenção
- Atualizações Contínuas: Inclusão de novas funcionalidades e bases de dados
- Precedentes Exitosos: Adotado com sucesso pela SENASP, RFB, TCDF e MPDFT
- Conformidade Garantida: Aderência a padrões nacionais e internacionais de segurança e privacidade

11. Análise comparativa de custos (TCO)

A contratação será de prestação de serviços continuados de OSINT e Social Listening com foco em contrainteligência e monitoramento da surface, deep e dark web.

Componentes:

- Plataforma SaaS com IA e agentes de IA Generativa, PLN e análise preditiva.
- Equipe técnica especializada (ver perfis abaixo).
- Relatórios diários, semanais, mensais e *ad hoc*.
- Monitoramento de ativos especificados no Edital de contratação e mediante assinatura de Termo de Compromisso e Manutenção de Sigilo (TCMS) após a fase licitatória.
- Alertas em tempo real.
- Treinamento e transferência de conhecimento para as equipes do BCB.

Abaixo segue a tabela com o detalhamento da estimativa de custos para a contratação do serviço:

Item	Descrição do Perfil	Salário de Referência (R$)	Fator-K	% Alocação	Custo Unitário Mensal (R$)	Custo Proporcional (R$)
1	Analista de OSINT Sênior (ASEG-03)	15.056,97	1,95	25%	29.361,09	7.340,27
2	Gerente de Projeto OSINT (GERSEG)	21.333,33	1,93	40,00%	41.173,33	16.469,33
3	Coordenador de Contrainteligência (GERINF)	17.851,64	1,94	25%	34.632,18	8.658,05
4	Analista de OSINT Júnior (ASEG-01)	6.966,67	2,05	70%	14.281,67	9.997,17
5	Especialista em Social Listening (ASISA-03)	11.283,00	1,98	100%	22.340,34	22.340,34
6	Especialista em Segurança Cibernética (ASEG-03)	15.056,97	1,95	40%	29.361,09	11.744,44
—	Total Estimado Mensal	—	—	—	—	R$ 76.549,60

11.1 Cálculo dos Custos Totais de Propriedade (TCO)

Item	Perfil Profissional	Custo Mensal (R$)	Custo Anual (R$)
1	Analista de OSINT Sênior (25%)	R$ 7.340,27	R$ 88.083,27
2	Gerente de Projeto OSINT (40%)	R$ 16.469,33	R$ 197.631,97
3	Coordenador de Contrainteligência (25%)	R$ 8.658,05	R$ 103.896,54
4	Analista de OSINT Sênior (70%)	R$ 9.997,17	R$ 119.966,06
5	Especialista em Social Listening (100%)	R$ 22.340,34	R$ 268.084,08
6	Especialista em Segurança Cibernética (40%)	R$ 11.744,44	R$ 140.933,24
—	Total Estimado Mensal	R$ 76.549,60	—
—	Total Estimado Anual	—	R$ 918.595,20

12. Descrição da solução de TIC a ser contratada

Após a análise comparativa das alternativas disponíveis no mercado e a avaliação técnica e econômica das soluções identificadas, optou-se pela contratação de uma solução integrada de inteligência de fontes abertas (OSINT) e Social Listening, na modalidade SaaS (Software como Serviço), com suporte especializado e equipe técnica multidisciplinar.

A solução escolhida se destaca por reunir, em um único contrato, os seguintes elementos:

- Plataforma tecnológica SaaS com funcionalidades avançadas de coleta, análise e visualização de dados provenientes da surface web, deep web e dark web, incluindo redes sociais, fóruns, canais criptografados e repositórios públicos;
- Capacidades analíticas baseadas em inteligência artificial, como análise de sentimento, PLN multilíngue, detecção de padrões anômalos, análise de redes e modelos preditivos;
- Equipe técnica especializada, composta por perfis profissionais mistos (Analistas OSINT, Especialistas em Social Listening, Segurança Cibernética, Cloud e Contrainteligência), conforme Portaria SGD/MGI nº 6.680/2024, com alocação proporcional e otimizada;
- Console de acesso para até 14 usuários intercambiáveis, com controle de credenciais e níveis de acesso hierarquizados;
- Produtos de contrainteligência como relatórios diários, semanais e mensais, alertas em tempo real e análises sob demanda;
- Transferência de conhecimento por meio de treinamentos periódicos, capacitação técnica e workshops de atualização;
- Conformidade com a LGPD, com mecanismos de segurança como criptografia, autenticação multifator, rastreabilidade e segregação lógica;
- Integração com sistemas internos do BCB via APIs padronizadas e exportação de dados em formatos interoperáveis (CSV, JSON, PDF etc.);
- Suporte técnico especializado, manutenção preventiva e corretiva, e atualizações contínuas da plataforma durante a vigência contratual.

A escolha dessa solução se justifica por sua especialização comprovada, rapidez de implementação, aderência aos requisitos técnicos e legais, escalabilidade operacional e custo-benefício otimizado. Além disso, trata-se da única alternativa capaz de atender integralmente aos requisitos funcionais e de segurança definidos pelo Banco Central do Brasil, conforme evidenciado na análise técnica detalhada e na memória de cálculo do TCO.

13. Estimativa de custo total da contratação

Valor (R$): 918.595,20

Efetuada a escolha da solução SaaS especializada em OSINT e Social Listening, com equipe técnica multidisciplinar e plataforma integrada, estima-se o custo total da contratação com base na composição de perfis profissionais, fator-K, alocação percentual e vigência contratual de 12 meses.

A seguir, apresenta-se a composição detalhada dos itens da solução, conforme planilha de custos e memória de cálculo:

Item	Descrição	Quantidade	Valor Unitário Mensal (R$)	Valor Total Anual (R$)
1	Analista de OSINT Sênior (25%)	1	R$ 7.340,27	R$ 88.083,27
2	Gerente de Projeto OSINT (40%)	1	R$ 16.469,33	R$ 197.631,97
3	Coordenador de Contrainteligência (25%)	1	R$ 8.658,05	R$ 103.896,54
4	Analista de OSINT Sênior (70%)	1	R$ 9.997,17	R$ 119.966,06
5	Especialista em Social Listening (100%)	1	R$ 22.340,34	R$ 268.084,08
6	Especialista em Segurança Cibernética (40%)	1	R$ 11.744,44	R$ 140.933,24
—	**Total Estimado**	**3 pessoas**	**R$ 76.549,60**	**R$ 918.595,20**

14. Justificativa técnica da escolha da solução

A solução escolhida — contratação de serviço continuado de OSINT (Open Source Intelligence) e Social Listening na modalidade SaaS com equipe técnica especializada — foi considerada a mais adequada após análise técnica, funcional e econômica das alternativas disponíveis.

A escolha se justifica pelos seguintes benefícios:

- Eficácia: a solução atende integralmente aos requisitos funcionais definidos pelo Banco Central do Brasil, permitindo o monitoramento contínuo e em tempo real de ameaças digitais, com cobertura da surface, deep e dark web, e entrega de produtos de contrainteligência acionável (relatórios, alertas, análises sob demanda).
- Eficiência: a contratação na modalidade SaaS elimina a necessidade de aquisição de infraestrutura própria, reduzindo custos operacionais e de manutenção, além de permitir rápida implementação e escalabilidade.

- Efetividade: a solução contribui diretamente para os objetivos estratégicos do BCB, como a proteção da imagem institucional, a antecipação de riscos e a segurança de ativos críticos, conforme previsto no Plano Diretor de Segurança (PDS 2024–2029).
- Economicidade: a composição da equipe técnica com perfis mistos e alocação proporcional (com base na Portaria SGD/MGI nº 6.680/2024) permitiu otimizar os custos sem comprometer a qualidade dos serviços, resultando em um custo total estimado compatível com o orçamento disponível.

Além disso, a solução apresenta ganhos técnicos relevantes, como:

- Alta performance analítica com uso de inteligência artificial e PLN;
- Interface intuitiva e interoperabilidade com sistemas internos via API;
- Segurança robusta com autenticação multifator, criptografia e rastreabilidade;
- Atualizações contínuas e suporte técnico especializado durante toda a vigência contratual.

14.1 Do Parcelamento da Contratação Decorrente de Aspectos Técnicos

Não se aplica parcelamento da contratação por aspectos técnicos.

A solução é ofertada de forma integrada, combinando plataforma tecnológica, equipe especializada e serviços de contrainteligência em um único contrato. O fracionamento técnico da contratação comprometeria a interoperabilidade entre os componentes, a rastreabilidade das análises e a responsabilização contratual, além de gerar riscos operacionais e de segurança.

A contratação unificada garante maior controle, padronização dos serviços, aderência aos requisitos de confidencialidade e sigilo institucional, e facilita a gestão contratual e a fiscalização técnica.

15. Justificativa econômica da escolha da solução

A solução escolhida apresenta vantagens econômicas significativas em relação às demais alternativas analisadas, tanto sob a ótica do custo total de propriedade (TCO) quanto da racionalização de recursos públicos.

A contratação de serviço continuado de OSINT e Social Listening na modalidade SaaS, com equipe técnica especializada e plataforma integrada, permite:

- Redução de custos indiretos com infraestrutura, licenciamento perpétuo, manutenção e suporte técnico, que seriam necessários em soluções on-premise ou desenvolvidas internamente;
- Eliminação de riscos de obsolescência tecnológica, uma vez que a solução SaaS inclui atualizações contínuas e evolutivas sem custo adicional;
- Aproveitamento de economia de escala, com composição de equipe baseada em perfis mistos e alocação proporcional, conforme Portaria SGD/MGI nº 6.680/2024, o que permitiu manter o custo mensal dentro do orçamento disponível;
- Custo total estimado previsível e estável, com valor mensal fixado em R$ 76.549,60 e custo total para 180 meses de R$ 13.778.928,00, conforme memória de cálculo consolidada;
- Melhor relação custo-benefício, considerando que a solução atende integralmente aos requisitos técnicos, legais e estratégicos do BCB, com menor risco operacional e maior agilidade de implementação.

Além disso, a análise de benchmarking com contratações similares na Administração Pública Federal demonstrou que soluções com escopo semelhante apresentaram valores superiores, especialmente quando envolviam licenças perpétuas, desenvolvimento interno ou múltiplos contratos fragmentados.

15.1 O Parcelamento da Contração Decorrente de Aspectos Econômicos

Não se aplica o parcelamento da contratação por aspectos econômicos.

A solução de TIC escolhida — composta por plataforma SaaS integrada e equipe técnica especializada — apresenta ganhos de escala e economicidade justamente por ser contratada de forma unificada. A fragmentação da contratação em múltiplos itens ou fornecedores comprometeria a eficiência operacional, aumentaria os custos administrativos e dificultaria a gestão contratual.

Além disso, a composição da equipe com perfis mistos e alocação proporcional permitiu otimizar os custos mensais, mantendo o valor total da contratação dentro do orçamento estimado. A contratação em lote único também assegura:

- Previsibilidade orçamentária ao longo dos 12 meses de vigência;
- Redução de riscos de variação de preços e encargos indiretos;
- Simplificação dos processos de fiscalização e pagamento;
- Maior controle sobre a qualidade e a continuidade dos serviços prestados.

Portanto, sob a ótica econômica, a contratação integrada é a alternativa mais vantajosa para a Administração, assegurando a melhor relação custo-benefício e aderência ao princípio da economicidade previsto na Lei nº 14.133/2021.

16. Benefícios a serem alcançados com a contratação

A contratação da solução integrada de OSINT (Open Source Intelligence) e Social Listening proporcionará ao Banco Central do Brasil uma série de benefícios estratégicos, operacionais e institucionais, alinhados aos princípios da eficácia, eficiência, efetividade e economicidade.

Entre os principais resultados esperados, destacam-se:

- Aprimoramento da capacidade de antecipação de riscos: a solução permitirá a identificação proativa de ameaças físicas e digitais, campanhas de desinformação, vazamentos de dados e comportamentos hostis direcionados à instituição, com base em fontes abertas e ambientes da deep e dark web;
- Fortalecimento da segurança institucional: por meio do monitoramento contínuo de ativos críticos (instalações, operações e reputação), a solução contribuirá para a proteção da imagem do BCB e a continuidade de suas operações estratégicas;
- Aumento da produtividade analítica: com o uso de inteligência artificial, análise de sentimento, PLN e dashboards interativos, a equipe de contrainteligência poderá produzir relatórios mais precisos, em menor tempo e com maior valor agregado;
- Redução de custos operacionais e tecnológicos: a adoção do modelo SaaS elimina a necessidade de aquisição de infraestrutura própria, reduz encargos com manutenção e garante atualizações contínuas sem custo adicional;
- Maior prontidão e agilidade na resposta a incidentes: com alertas em tempo real e relatórios *ad hoc*, a solução permitirá reações rápidas a eventos críticos, reduzindo impactos reputacionais e operacionais;
- Transferência de conhecimento e capacitação interna: a contratação inclui treinamentos periódicos e workshops técnicos, promovendo o desenvolvimento de competências internas e reduzindo a dependência de fornecedores externos;
- Conformidade com a LGPD e padrões de segurança da informação: a solução adota controles robustos de proteção de dados, rastreabilidade e autenticação, garantindo aderência às normas regulatórias e às diretrizes do Plano Diretor de Segurança (PDS 2024–2029).

Esses benefícios, combinados à previsibilidade orçamentária e à eficiência na gestão contratual, justificam plenamente a contratação da solução proposta como a alternativa mais vantajosa para a Administração.

17. Providências a serem Adotadas

Para viabilizar a celebração do contrato e garantir a adequada execução dos serviços contratados, serão adotadas as seguintes providências pela Administração:

1. Designação formal da equipe de fiscalização contratual, com a nomeação de fiscais técnico e administrativo, conforme previsto na Lei nº 14.133/2021 e nas orientações da IN SEGES/ME nº 05/2017;
2. Capacitação dos fiscais designados, com foco em:
    - Monitoramento de entregas e produtos de contrainteligência;
    - Avaliação de conformidade técnica da plataforma e dos relatórios;
    - Gestão de riscos contratuais e controle de indicadores de desempenho;
3. Adequação do ambiente organizacional, incluindo:
    - Provisão de infraestrutura mínima para acesso seguro à plataforma contratada (estações de trabalho, conectividade, autenticação);
    - Definição de perfis de acesso e controle de credenciais para os 14 usuários intercambiáveis previstos;
4. Elaboração do Plano de Fiscalização Contratual, com definição de marcos de verificação, critérios de aceite e periodicidade de reuniões de acompanhamento;
5. Integração com áreas correlatas, como segurança institucional, tecnologia da informação e comunicação, e gestão de riscos, para garantir alinhamento estratégico e operacional da solução contratada;
6. Formalização da dotação orçamentária, com empenho dos recursos necessários para a contratação, conforme previsto no planejamento orçamentário da unidade requisitante.

Essas providências visam assegurar a efetividade da contratação, a conformidade com os normativos vigentes e a obtenção dos resultados esperados com a solução de OSINT e Social Listening.

18. Declaração de Viabilidade

Esta equipe de planejamento declara **viável** esta contratação.

18.1. Justificativa da Viabilidade

18.1 Justificativa

A presente contratação foi considerada viável após análise técnica, funcional e econômica das alternativas disponíveis no mercado, conforme estabelecido nos artigos 11 e 18 da Lei nº 14.133/2021 e na Instrução Normativa SGD/ME nº 94/2022.

A alternativa escolhida — contratação de solução integrada de OSINT (Open Source Intelligence) e Social Listening na modalidade SaaS, com equipe técnica especializada — foi selecionada por atender integralmente aos requisitos estratégicos, operacionais e legais do Banco Central do Brasil, com base nos seguintes fundamentos:

- Análise técnica-funcional: a solução apresenta aderência total aos requisitos de monitoramento de ameaças em ambientes digitais (surface, deep e dark web), com funcionalidades avançadas de inteligência artificial, análise de sentimento, PLN, dashboards interativos e integração via API com sistemas internos;
- Análise econômica: a composição de equipe com perfis mistos e alocação proporcional, conforme a Portaria SGD/MGI nº 6.680 /2024, permitiu manter o custo mensal dentro do orçamento disponível, com TCO previsível e economicamente vantajoso em relação a outras soluções analisadas;
- Viabilidade operacional: a solução é de rápida implementação, não exige aquisição de infraestrutura própria e inclui suporte técnico, atualizações contínuas e transferência de conhecimento.

A contratação proporcionará benefícios expressivos à instituição, conforme as seguintes dimensões:

- Eficácia: a solução permitirá atingir os objetivos definidos, entregando os produtos de contrainteligência (relatórios, alertas, análises) com qualidade e dentro dos prazos estabelecidos;

Efetividade: contribuirá diretamente para a proteção da imagem institucional, a segurança de ativos críticos e a antecipação de riscos, alinhando-se ao Plano Diretor de Segurança (PDS 2024–2029);

- Eficiência: a contratação foi estruturada para fazer mais com menos, otimizando recursos humanos e tecnológicos por meio de alocação proporcional e uso de tecnologia SaaS;
- Economicidade: a solução apresenta a melhor relação custo-benefício, considerando o escopo, os resultados esperados e a sustentabilidade orçamentária ao longo dos 12 meses de vigência.

Dessa forma, a contratação é plenamente viável e recomendada, sendo a alternativa que melhor atende ao interesse público, à estratégia institucional e aos princípios da nova Lei de Licitações e Contratos.

19. Responsáveis

Todas as assinaturas eletrônicas seguem o horário oficial de Brasília e fundamentam-se no §3º do Art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

AROLDO FERRAZ

Membro da comissão de contratação

SHYRLEY SILVA DA SILVA

Membro da comissão de contratação

RENATO FISCHER

Membro da comissão de contratação